

TWO ADDITION THEOREMS ON POLYNOMIALS OF PRIME VARIABLES

HONGZE LI AND HAO PAN

1. INTRODUCTION

Recently, Khalfalah and Szemerédi [7] proved the following theorem, which was conjectured by Erdős, Roth, Sárközy and Sós [3]:

Theorem 1.1. *Let ψ be a polynomial with integral coefficients and positive leading coefficient. Suppose that $\psi(1)\psi(0)$ is even. Then for any m -coloring of all positive integers (i.e., partitioning \mathbb{Z}^+ into m disjoint non-empty subsets), there exist monochromatic distinct x, y such that $x + y = \psi(z)$ for an integer z .*

In particular, if all positive integers are colored with m -colors, then there exists a monochromatic pair x, y with $x \neq y$ such that $x + y$ is a perfect square.

On the other hand, suppose that ψ is a polynomial with rational coefficients and zero constant term, in [9] Li and Pan proved that for any subset A of positive integers with

$$\limsup_{x \rightarrow \infty} \frac{|A \cap [1, x]|}{x} > 0,$$

there exist $x, y \in A$ and a prime p such that $x - y = \psi(p - 1)$. This commonly generalizes two well-known results of Furstenberg [4] and Sárközy [10, 11].

Define

$$\lambda_{b,W}(x) = \begin{cases} \frac{\phi(W)}{W} \log(Wx + b) & \text{if } Wx + b \text{ is prime,} \\ 0 & \text{otherwise,} \end{cases}$$

where ϕ is the Euler totient function and

$$\Lambda_{b,W} = \{x : Wx + b \text{ is prime}\}$$

for $1 \leq b \leq W$ with $(b, W) = 1$. In the present paper, our main result is the following theorem:

Theorem 1.2. *Let m, b_0, W_0 be positive integers satisfying $b_0 \leq W_0$ and $(b_0, W_0) = 1$. Let $\psi(x)$ be a polynomial with integral coefficients and positive leading coefficient satisfying that*

$$\begin{cases} \psi(1) \text{ or } \psi(0) \text{ is even} & \text{if } 2 \mid W_0, \\ \psi(b_0 - 1) \text{ is even} & \text{if } 2 \nmid W_0. \end{cases}$$

2000 *Mathematics Subject Classification.* Primary 11P32; Secondary 05D99, 11P55.

This work was supported by the National Natural Science Foundation of China (Grant No. 10471090).

Suppose that all positive integers are colored with m colors. Then there exist distinct monochromatic x, y such that $x + y = \psi(z)$ where $z \in \Lambda_{b_0, W_0}$.

We shall use one of Green's ingredients in his proof of Roth's theorem in primes. The key of Green's proof is a transference principle (which was greatly developed in [6]), i.e., transferring a subset of primes with positive relative density to a subset of $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ with positive density, where N is a large prime. In the proof of Theorem 1.2, we shall transfer one subset of $\{\psi(z) : z \in \Lambda_{b, W}\}$ to a subset of $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ with the density very close to 1.

Theorem 1.3. *Let m, b_0, W_0 be positive integers satisfying $b_0 \leq W_0$ and $(b_0, W_0) = 1$. Let $\psi(x)$ be a polynomial with integral coefficients and positive leading coefficient satisfying that*

$$\begin{cases} \psi(1) \text{ or } \psi(0) \text{ is even} & \text{if } 2 \mid W_0, \\ \psi(b_0 - 1) \text{ is even} & \text{if } 2 \nmid W_0. \end{cases}$$

Also, suppose that for each prime p , there exists $1 \leq c_p \leq p$ such that both $W_0 c_p + b_0$ and $\frac{1}{2}\psi(c_p)$ are not divisible by p . Then for any m -coloring of all primes, there exist distinct monochromatic primes x, y such that $x + y = \psi(z)$ where $z \in \Lambda_{b_0, W_0}$.

Let us explain why the existence of c_p is necessary. Assume that there exists a prime p such that c_p doesn't exist. That is, for each $1 \leq c \leq p$, either $W_0 c + b_0$ or $\frac{1}{2}\psi(c)$ is divisible by p . Then we may partition the set of all primes into $3p$ disjoint sets X_1, \dots, X_{3p} with

$$X_j = \{x \text{ is prime} : x \leq \psi((p - b_0)/W_0)/2, x \equiv j \pmod{p}\},$$

$$X_{p+j} = \{x \text{ is prime} : x > \psi((p - b_0)/W_0)/2, x \equiv j \pmod{p}\}$$

and

$$X_{2p+j} = \{x \text{ is prime} : \psi((p - b_0)/W_0)/2 < x \leq \psi((p - b_0)/W_0), x \equiv j \pmod{p}\}.$$

for $j = 1, 2, \dots, p$. We claim that for each $1 \leq j \leq 3p$, the set

$$\{(x, y, z) : x, y \in X_j, z \in \Lambda_{b_0, W_0}, x \neq y, x + y = \psi(z)\}$$

is empty.

In fact, notice that now p divides one of $W_0 z + b_0$ and $\frac{1}{2}\psi(z)$ since c_p doesn't exist. If p divides $W_0 z + b_0$, we must have $W_0 z + b_0 = p$ since $z \in \Lambda_{b_0, W_0}$. But it is easy to see that for $1 \leq j \leq p$

$$\max\{x + y : x, y \in X_j, x \neq y\} < 2 \cdot \psi((p - b_0)/W_0)/2 = \psi(z),$$

and for $p + 1 \leq j \leq 3p$

$$\min\{x + y : x, y \in X_j, x \neq y\} > 2 \cdot \psi((p - b_0)/W_0)/2 = \psi(z).$$

So it is impossible that

$$\psi(z) \in X_j + X_j := \{x + y : x, y \in X_j, x \neq y\}$$

for any $1 \leq j \leq 3p$.

On the other hand, suppose that p divides $\frac{1}{2}\psi(z)$. Note that for any $1 \leq j \leq 3p$ and $x, y \in X_j$, $x \equiv y \equiv j \pmod{p}$. So if $x + y = \psi(z)$, then we must have

$x \equiv y \equiv 0 \pmod{p}$. Thus we have $x = y = p$ since x, y are both primes. This also concludes that $\psi(z) \notin X_j + X_j$ for each j .

2. PROOF OF THEOREM 1.2

Assume that n is a sufficiently large integer, and

$$\{1, 2, \dots, n\} = X_1 \cup \dots \cup X_m$$

where $X_i \cap X_j = \emptyset$ if $i \neq j$.

Lemma 2.1. *Let p be a prime. Let $h(x)$ be a non-zero polynomial over \mathbb{Z}_p . Suppose that $S \subseteq \mathbb{Z}_p$ and $|S| \geq \deg h + 1$. Then there exists $b \in S$ such that $h(b) \not\equiv 0 \pmod{p}$.*

Proof. This lemma easily follows from the fact that

$$|\{x \in \mathbb{Z}_p : h(x) = 0\}| \leq \deg h,$$

since $h(x)$ doesn't vanish over \mathbb{Z}_p . \square

Suppose $\psi(x) = a_1 x^k + \dots + a_k x + a_0$ be a polynomial with integral coefficients. Let $\Psi = \max\{(k+1)W_0, |a_1|, \dots, |a_k|\}$. Let ψ' denote the derivative of ψ . Then for any prime $p > \Psi$, by Lemma 2.1, there exists $1 \leq b_p \leq p-1$ with $b_p \equiv b_0 \pmod{W_0}$ such that $(\psi'((b_p - b_0)/W_0), p) = 1$. And for each prime $p \leq \Psi$, we may choose $b_p \geq 1$ with $p \nmid b_p$ such that $b_p \equiv b_0 \pmod{W_0}$ and $\psi'((b_p - b_0)/W_0) > 0$. In particular, we may assume that $\psi((b_2 - b_0)/W_0)$ is even if $2 \mid W_0$. Let

$$K = \prod_{\substack{p \text{ prime} \\ p \leq \Psi}} p^{\nu_p(\psi'((b_p - b_0)/W_0))},$$

where $\nu_p(x) = \max\{v \in \mathbb{Z} : p^v \mid x\}$.

Let $\kappa = 10^{-4} K^{-1} m^{-1}$. Let $w = \lfloor \log \log \log \log n \rfloor$ and

$$W = \prod_{\substack{p \text{ prime} \\ p \leq w}} p^w.$$

Without loss of generality, we may assume that $w \geq \Psi$. Suppose that N is a prime in the interval $(2n/W, (2 + \kappa)n/W]$. Thanks to the prime number theorem, such prime N always exists whenever n is sufficiently large. By the Chinese remainder theorem, there exists $0 \leq b \leq W - 1$ such that for each prime $p \leq w$

$$W_0 b + b_0 \equiv b_p \pmod{p^{w + \nu_p(W_0)}},$$

since $b_p \equiv b_0 \pmod{W_0}$. Clearly $(W_0 b + b_0, W W_0) = 1$. We claim that $\psi(b)$ is even. In fact, when W_0 is odd, $b \equiv b_2 - b_0 \equiv b_0 - 1 \pmod{2}$. And if W_0 is even, we also have $2 \mid \psi(b)$ since $b \equiv (b_2 - b_0)/W_0 \pmod{2}$.

Define

$$\psi_{b,W}(x) = \frac{\psi(Wx + b) - \psi(b)}{W}.$$

Let $M = \max\{x \in \mathbb{N} : \psi_{b,W}(x) < KN\}$. Let B be a sufficiently large positive constant (only depending on k). Let

$$\mathfrak{M}_{a,q} = \{\alpha \in \mathbb{T} : |\alpha q - a| \leq (\log M)^B / \psi_{b,W}(M)\},$$

$$\mathfrak{M} = \bigcup_{\substack{1 \leq a \leq q \leq (\log M)^B \\ (a, q) = 1}} \mathfrak{M}_{a, q}$$

and $\mathfrak{m} = \mathbb{T} \setminus \mathfrak{M}$, where $\mathbb{T} = \mathbb{R}/\mathbb{Z}$.

Lemma 2.2. *For $\alpha \in \mathfrak{M}_{a, q}$,*

$$\begin{aligned} & \sum_{x=1}^M \psi_{b, W}^\Delta(x-1) \lambda_{W_0 b + b_0, W W_0}(x) e(\alpha \psi_{b, W}(x)) \\ &= \frac{\phi(W W_0)}{\phi(W W_0 q)} \sum_{\substack{1 \leq r \leq q \\ (W W_0 r + W_0 b + b_0, q) = 1}} e(a \psi_{b, W}(r)/q) \sum_{x=1}^{\psi_{b, W}(M)} e((\alpha - a/q) \psi_{b, W}(x)) \\ &+ O(\psi_{b, W}(M) (\log M)^{-B}), \end{aligned}$$

where $\psi_{b, W}^\Delta(x) = \psi_{b, W}(x+1) - \psi_{b, W}(x)$.

Lemma 2.3. *Suppose that $U \geq e^{a_1 W^k}$. For any $A > 0$, there is a $B = B(A, k) > 0$ such that,*

$$\sum_{x=1}^N \lambda_{b, W}(x) e(\alpha \psi(x)) \ll_B N (\log N)^{-A}$$

provided that $|\alpha - a/q| \leq q^{-2}$ with $1 \leq a \leq q$, $(a, q) = 1$ and $(\log N)^B \leq q \leq \psi(N) (\log N)^{-B}$.

Lemma 2.2 is the immediate consequence of Lemmas 2.3 and 2.4 of [9]. The proof of Lemma 2.3 is standard but too long, so we omit the details here. And the readers may refer to [9] for the proof.

Clearly $\psi_{b, W}$ is positive and strictly increasing on $[1, M]$ provided that W is sufficiently large. Define

$$\mathfrak{a}(x) = \begin{cases} \psi_{b, W}^\Delta(z-1) \lambda_{W_0 b + b_0, W W_0}(z) / \psi_{b, W}(M) & \text{if } x = \psi_{b, W}(z) \text{ for a } 1 \leq z \leq M, \\ 0 & \text{otherwise.} \end{cases}$$

For any $f : \mathbb{Z}_N \rightarrow \mathbb{C}$, define

$$\tilde{f}(r) = \sum_{x=1}^N f(x) e(-xr/N).$$

Lemma 2.4. *For any $0 \neq r \in \mathbb{Z}_N$,*

$$|\tilde{\mathfrak{a}}(r)| \leq C_1 K w^{-\frac{1}{k(k+3)}}, \quad (2.1)$$

where C_1 is a constant (only depending on k).

Proof. If $r/N \in \mathfrak{m}$, then by Lemma 2.3 and partial summation,

$$\tilde{\mathfrak{a}}(r) = \frac{1}{\psi_{b, W}(M)} \sum_{z=1}^M \psi_{b, W}^\Delta(z-1) \lambda_{W_0 b + b_0, W W_0}(z) e(-\psi_{b, W}(z)r/N) \ll (\log M)^{-1}.$$

Suppose that $r/N \in \mathfrak{M}_{a,q}$. Then by Lemma 2.2

$$\begin{aligned} & \frac{1}{\psi_{b,W}(M)} \sum_{z=1}^M \psi_{b,W}^\Delta(z-1) \lambda_{W_0b+b_0, WW_0}(z) e(-\psi_{b,W}(z)r/N) \\ &= \frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{\substack{1 \leq s \leq q \\ (WW_0s+W_0b+b_0,q)=1}} e(-\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) \\ &+ O((\log M)^{-B}) \end{aligned}$$

Notice that the leading coefficient of $\psi_{b,W}(x)$ is $a_1 W^{k-1}$, and the coefficient of x^1 in $\psi_{b,W}(x)$ coincides with

$$\psi'_{b,W}(0) = \frac{d}{dx} \left(\frac{\psi(Wx+b) - \psi(b)}{W} \right) \Big|_{x \rightarrow 0} = \frac{d\psi(x)}{dx} \Big|_{x \rightarrow b} = \psi'(b).$$

Also, clearly for each prime $p \leq w$, $\psi'(b) \equiv \psi'((b_p - b_0)/W_0) \pmod{p^w}$ since $W_0b + b_0 \equiv b_p \pmod{p^{w+\nu_p(W_0)}}$. Therefore when w is sufficiently large, we have

$$(\psi'(b), a_1 W^{k-1}) = (\psi'(b), W) = \prod_{p \leq \Psi} p^{\nu_p(\psi'((b_p - b_0)/W_0))} = K.$$

Thus by Lemma 2.7 of [9],

$$\sum_{\substack{1 \leq s \leq q \\ (WW_0s+W_0b+b_0,q)=1}} e(\psi_{b,W}(s)a/q) \ll K q^{1 - \frac{1}{k(k+2)}}.$$

Let q_2 be the largest divisor of q prime to W and $q_1 = q/q_2$. If $q \nmid W$, then either $q_2 > w$ or $q \geq 2^w$. Hence

$$\begin{aligned} & \frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{\substack{1 \leq s \leq q \\ (WW_0s+W_0b+b_0,q)=1}} e(\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) \\ & \ll \frac{K q^{1 - \frac{1}{k(k+2)}}}{q_1 \phi(q_2) \psi_{b,W}(M)} \left| \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) \right| \\ & \ll K w^{-\frac{1}{k(k+3)}}. \end{aligned}$$

Below assume that $q \mid W$. Since W divides the coefficients of x^i in $\psi_{b,W}(x)$ for $2 \leq i \leq k$, we have

$$\sum_{\substack{1 \leq s \leq q \\ (WW_0s+W_0b+b_0,q)=1}} e(\psi_{b,W}(s)a/q) = \sum_{1 \leq s \leq q} e(\psi'(b)sa/q) = \begin{cases} q & \text{if } q \mid (\psi'(b), W) = K, \\ 0 & \text{otherwise.} \end{cases}$$

Now suppose that $q \mid K$. Since $KN - \psi_{b,W}(M) \leq \psi_{b,W}^\Delta(M)$, then

$$\begin{aligned} \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) &= \sum_{x=1}^{KN} e(x(r/N - a/q)) + O(\psi_{b,W}^\Delta(M)) \\ &= O(\psi_{b,W}^\Delta(M)). \end{aligned}$$

This concludes that if $q \mid W$ then

$$\begin{aligned} &\frac{\phi(WW_0)}{\phi(WW_0q)\psi_{b,W}(M)} \sum_{\substack{1 \leq s \leq q \\ (WW_0s + W_0b + b_0, q) = 1}} e(\psi_{b,W}(s)a/q) \sum_{x=1}^{\psi_{b,W}(M)} e(x(r/N - a/q)) \\ &= O((\log M)^{-B}). \end{aligned}$$

□

By the pigeonhole principle, there exists $1 \leq i \leq m$ such that

$$|\{x \in X_i \cap [\psi(W), n] : x \equiv \psi(b)/2 \pmod{KW}\}| \geq \frac{n}{mKW} - \psi(W) \geq \frac{N}{4mK}.$$

Without loss of generality, we may assume that X_1 is such a set. Let

$$A = \{(x - \psi(b)/2)/W : x \in X_1 \cap [\psi(W), n] : x \equiv \psi(b)/2 \pmod{KW}\}.$$

Suppose that there exist $x', y' \in A$ and $z' \in \Lambda_{W_0b+b_0, WW_0}$ such that $x' + y' = \psi_{b,W}(z')$. Then letting $x = Wx' + \psi(b)/2$, $y = Wy' + \psi(b)/2 \in X_1$ and $z = Wz' + b \in \Lambda_{b_0, W_0}$, we have $x + y = \psi(z)$.

Below we consider A as a subset of \mathbb{Z}_N . We claim that if $x, y \in A$ and $z \in \Lambda_{W_0b+b_0, WW_0} \cap [1, M]$ satisfy $x + y = \psi_{b,W}(z)$ in \mathbb{Z}_N , then the equality also holds in \mathbb{Z} . Suppose that $x + y = \psi_{b,W}(z) - lN$ for an integer l . Then $0 \leq l < K$ since $n/W < N/2$ and $\psi_{b,W}(z) < KN$. Notice that K divides $x + y$ and all coefficients of $\psi_{b,W}$. We must have $K \mid l$, whence $l = 0$. Furthermore, we may consider \mathbf{a} as a function over \mathbb{Z}_N , i.e.,

$$\mathbf{a}(x) = \begin{cases} \frac{\psi_{b,W}^\Delta(z-1)}{\psi_{b,W}(M)} \lambda_{W_0b+b_0, WW_0}(z) & \text{if } x = \psi_{b,W}(z) \text{ in } \mathbb{Z}_N \text{ for a } 1 \leq z \leq M, \\ 0 & \text{otherwise.} \end{cases}$$

This function is well-defined. In fact, assume that $1 \leq z_1, z_2 \leq M$ and $\psi_{b,W}(z_1) = \psi_{b,W}(z_2)$ in \mathbb{Z}_N . Then $\psi_{b,W}(z_1) = \psi_{b,W}(z_2) + lN$ in \mathbb{Z} where $|l| < K$. But $\psi_{b,W}(z_1) \equiv \psi_{b,W}(z_2) \pmod{K}$, so $l = 0$ and $z_1 = z_2$.

Let η and ϵ be two positive real numbers to be chosen later. Let

$$\mathcal{R} = \{r \in \mathbb{Z}_N : |\tilde{\mathbf{a}}(r)| \geq \eta\}$$

and

$$\mathcal{B} = \{x \in \mathbb{Z}_N : \|xr/N\| \leq \epsilon \text{ for all } r \in \mathcal{R}\},$$

where $\|x\| = \min\{|x - z| : z \in \mathbb{Z}\}$. Define $\mathbf{b} = \mathbf{1}_{\mathcal{B}}/|\mathcal{B}|$ and $\mathbf{a}' = \mathbf{a} * \mathbf{b} * \mathbf{b}$, where $\mathbf{1}_{\mathcal{B}}(x) = 1$ or 0 according to whether $x \in \mathcal{B}$ or not and

$$f * g(x) = \sum_{y \in \mathbb{Z}_N} f(y)g(x - y).$$

Lemma 2.5. *If $\epsilon^{|\mathcal{R}|} \geq \kappa^{-1} C_1 K w^{-\frac{1}{k(k+3)}}$, then for any $x \in \mathbb{Z}_N$*

$$|\mathbf{a}'(x)| \leq \frac{1 + 2\kappa}{N}.$$

Proof. It is easy to see that $\widetilde{(f * g)} = \tilde{f} \cdot \tilde{g}$. By Lemma 2.2 for $\alpha = 0$ and Lemma 2.4,

$$\begin{aligned} |\mathbf{a}'(x)| &= \left| \frac{1}{N} \sum_r \tilde{\mathbf{a}}(r) \tilde{\mathbf{b}}(r)^2 e\left(\frac{xr}{N}\right) \right| \\ &\leq \frac{1}{N} |\tilde{\mathbf{b}}(0)|^2 \sum_{z=1}^M \frac{\psi_{b,W}^\Delta(z-1)}{\psi_{b,W}(M)} \lambda_{W_0 b + b_0, W W_0}(z) + \frac{1}{N} \sup_{r \neq 0} |\tilde{\mathbf{a}}(r)| \sum_{r \neq 0} |\tilde{\mathbf{b}}(r)|^2 \\ &\leq \frac{1 + \kappa}{N} + \frac{C_1 K w^{-\frac{1}{k(k+3)}}}{|\mathcal{B}|}. \end{aligned}$$

By the pigeonhole principle (cf. [12, Lemma 1.4]), we have $|\mathcal{B}| \geq \epsilon^{|\mathcal{R}|} N$. All are done. \square

Lemma 2.6.

$$\sum_{r \in \mathbb{Z}_N} |\tilde{\mathbf{a}}(r)|^\rho \leq C(\rho) K.$$

provided that $\rho \geq k2^{k+3}$, where $C(\rho)$ is a constant only depending on ρ .

Proof. Note that

$$\sum_{r \in \mathbb{Z}_N} |\tilde{\mathbf{a}}(r)|^\rho = \frac{1}{\psi_{b,W}(M)^\rho} \sum_{r \in \mathbb{Z}_N} \left| \sum_{z=1}^M \psi_{b,W}^\Delta(z-1) \lambda_{W_0 b + b_0, W W_0}(z) e(-\psi_{b,W}(z)r/N) \right|^\rho.$$

Thus Lemma 2.6 easily follows from Lemma 2.10 of [9]. \square

Lemma 2.7.

$$\begin{aligned} &\left| \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}(z) - \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}'(z) \right| \\ &\leq C_2 K (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N, \end{aligned}$$

where C_2 is a positive constant (only depending on k).

Proof. It is easy to see that

$$\sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}(z) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r)$$

and

$$\sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}'(z) = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r) \tilde{\mathbf{b}}(r)^2.$$

Hence

$$\begin{aligned} & \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}(z) - \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}'(z) \\ &= \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r) (1 - \tilde{\mathbf{b}}(r)^2). \end{aligned}$$

Let $\rho = k2^{k+3}$. If $r \in \mathcal{R}$, then by the proof of Lemma 6.7 of [5]

$$|1 - \tilde{\mathbf{b}}(r)^2| \leq 32\epsilon^2.$$

So

$$\left| \sum_{r \in \mathcal{R}} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r) (1 - \tilde{\mathbf{b}}(r)^2) \right| \leq |1 - \tilde{\mathbf{b}}(r)^2| \sum_{r \in \mathcal{R}} |\tilde{\mathbf{1}}_A(r)|^2 |\tilde{\mathbf{a}}(r)| \leq 64\epsilon^2 N^2 |\mathcal{R}|.$$

By Lemma 2.6 we have,

$$|\mathcal{R}| \leq \eta^{-\rho} \sum_{r \in \mathcal{R}} |\tilde{\mathbf{a}}(r)|^\rho \leq C(\rho) K \eta^{-\rho}.$$

Applying the Hölder inequality,

$$\begin{aligned} & \left| \sum_{r \notin \mathcal{R}} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r) (1 - \tilde{\mathbf{b}}(r)^2) \right| \\ & \leq \left| \sum_{r \notin \mathcal{R}} \tilde{\mathbf{1}}_A(r) \tilde{\mathbf{1}}_A(-r) \tilde{\mathbf{a}}(r) (1 - \tilde{\mathbf{b}}(r)^2) \right| \\ & \leq 2N^{\frac{2}{\rho+1}} \sup_{r \notin \mathcal{R}} |\tilde{\mathbf{a}}(r)|^{\frac{1}{\rho+1}} \left(\sum_{r \notin \mathcal{R}} |\tilde{\mathbf{1}}_A(r)|^2 \right)^{\frac{\rho}{\rho+1}} \left(\sum_{r \notin \mathcal{R}} |\tilde{\mathbf{a}}(r)|^\rho \right)^{\frac{1}{\rho+1}} \\ & \leq 2C(\rho)^{\frac{1}{\rho+1}} K^{\frac{1}{\rho+1}} \eta^{\frac{1}{\rho+1}} N^2, \end{aligned}$$

where we again use Lemma 2.6 in the last step. □

Lemma 2.8.

$$\sum_{\substack{x, y, z \in \mathbb{Z}_N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathbf{a}'(z) \geq \kappa^4 N.$$

Proof. Let

$$\mathfrak{A} = \{x \in \mathbb{Z}_N : \mathbf{a}'(x) \geq \kappa/N\}.$$

Then by Lemma 2.5

$$\frac{1+2\kappa}{N} |\mathfrak{A}| + \frac{\kappa}{N} (N - |\mathfrak{A}|) \geq \sum_{x \in \mathbb{Z}_N} \mathbf{a}'(x) = \sum_{x \in \mathbb{Z}_N} \mathbf{a}(x) \geq 1 - \kappa,$$

whence $|\mathfrak{A}| \geq (1 - 3\kappa)N$. Define

$$\nu_{A, A, -\mathfrak{A}}(x) = |\{(x_1, x_2, x_3) : x_1, x_2 \in A, x_3 \in \mathfrak{A}, x_1 + x_2 - x_3 = x\}|.$$

By Lemma 3.3 of [8], we know

$$\nu_{A,A,-\mathfrak{A}}(x) \geq (\min\{|A|, |\mathfrak{A}|, \frac{2|A| + |\mathfrak{A}| - N}{4}\})^3 N^{-1}.$$

for any $x \in \mathbb{Z}_N$. It follows that

$$\sum_{\substack{x,y,z \in \mathbb{Z}_N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathfrak{a}'(z) \geq \sum_{\substack{x,y \in A, z \in \mathfrak{A} \\ x+y=z}} \frac{\kappa}{N} = \frac{\kappa}{N} \nu_{A,A,-\mathfrak{A}}(0) \geq \kappa^4 N.$$

□

Combining Lemmas 2.7 and 2.8, we obtain that

$$\begin{aligned} & \sum_{\substack{1 \leq x,y,z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathfrak{a}(z) \\ & \geq \sum_{\substack{1 \leq x,y,z \leq N \\ x+y=z}} \mathbf{1}_A(x) \mathbf{1}_A(y) \mathfrak{a}'(z) - C_2 K (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N \\ & \geq \kappa^4 N - C_2 K (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N. \end{aligned}$$

We may choose sufficiently small η and ϵ such that

$$\epsilon^{C(k2^{k+3})K} \eta^{-k2^{k+3}} \geq \kappa^{-1} C_1 K w^{-\frac{1}{k(k+3)}}$$

and $C_2 K (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) \leq \kappa^4/2$, provided that w is sufficiently large. Thus

$$\sum_{\substack{x,y \in A, 1 \leq z \leq N \\ x \neq y, x+y=z}} \mathfrak{a}(z) \geq \sum_{\substack{x,y \in A, 1 \leq z \leq N \\ x+y=z}} \mathfrak{a}(z) - \sum_{1 \leq z \leq N} \mathfrak{a}(z) \geq \frac{\kappa^4}{3} N.$$

All are done. □

3. PROOF OF THEOREM 1.3

Let \mathcal{P} denote the set of all primes. Assume that $\mathcal{P} = X_1 \cup \dots \cup X_m$ where $X_i \cap X_j = \emptyset$ if $i \neq j$. Also, let $\kappa = 10^{-4} K^{-1} m^{-1}$.

Let $\Psi = \max\{(2k+1)W_0, |a_1|, \dots, |a_k|\}$. Then for a prime $p > \Psi$, by Lemma 2.1 we know that there exists $1 \leq b_p \leq p-1$ with $b_p \equiv b_0 \pmod{W_0}$ such that

$$\psi'((b_p - b_0)/W_0) \psi((b_p - b_0)/W_0) \not\equiv 0 \pmod{p}.$$

For a prime $p \leq \Psi$, we may choose $b_p \geq 1$ such that

$$b_p \equiv W_0 c_p + b_0 \pmod{pW_0}$$

and $\psi'((b_p - b_0)/W_0) > 0$. Let

$$K = \prod_{\substack{p \text{ prime} \\ p \leq \Psi}} p^{\nu_p(\psi'((b_p - b_0)/W_0))},$$

where $\nu_p(x) = \max\{v \in \mathbb{Z} : p^v \mid x\}$.

Suppose that n is a sufficiently large integer. Let $w = \lfloor \log \log \log \log n \rfloor$ and

$$W = \prod_{\substack{\text{prime} \\ p \leq w}} p^w.$$

Same as previous section, there exists $1 \leq b \leq W - 1$ such that

$$W_0 b + b_0 \equiv b_p \pmod{p^{w+\nu_p(W_0)}}$$

for each prime $p \leq w$. And also we know that $\psi(b)$ is even.

By the prime number theorem, we know

$$\sum_{\substack{1 \leq x \leq n, \\ x \equiv \psi(b)/2 \pmod{KW}, \\ x \text{ prime}}} \log x = \frac{(1 + o(1))n}{\phi(KW)}.$$

Hence in view of the pigeonhole principle, without loss of generality, we may assume that

$$\sum_{\substack{x \in X_1 \cap [\psi(W), n] \\ x \equiv \psi(b)/2 \pmod{KW}}} \log x \geq \frac{(1 - \kappa)n}{m\phi(KW)}.$$

Let N be a prime in $(2n/W, (2 + \kappa)n/W]$ and

$$A = \{(x - \psi(b)/2)/W : x \in X_1 \cap [\psi(W), n], x \equiv \psi(b)/2 \pmod{KW}\}.$$

Below we consider A as a subset of \mathbb{Z}_N . Similarly, if $x' + y' = \psi_{b,W}(z')$ holds in \mathbb{Z}_N for $x', y' \in A$ and $z' \in \Lambda_{W_0 b + b_0, WW_0}$, then we also have $x + y = \psi(z)$ holds in \mathbb{Z} where $x = Wx' + \psi(b)/2$, $y = Wy' + \psi(b)/2 \in X_1$ and $z = Wz' + b \in \Lambda_{b_0, W_0}$. Define $a = \mathbf{1}_A \lambda_{\psi(b)/2, KW}/N$. Clearly we have

$$\sum_{x=1}^N a(x) \geq \frac{1}{3mK}.$$

Lemma 3.1 (Bourgain [1, 2] and Green [5]).

$$\sum_{r=1}^N |\tilde{a}(r)|^\rho \leq C'(\rho)$$

for any $\rho > 2$.

Proof. See [5, Lemma 6.6]. □

Let

$$R = \{r \in \mathbb{Z}_N : |\tilde{a}(r)| \geq \eta\}$$

and

$$B = \{x \in \mathbb{Z}_N : \|xr/N\| \leq \epsilon \text{ for all } r \in R\}.$$

Define $\beta = \mathbf{1}_B/|B|$ and $a' = a * \beta * \beta$.

Lemma 3.2.

$$\left| \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} a(x)a(y)\mathfrak{a}(z) - \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} a'(x)a'(y)\mathfrak{a}'(z) \right| \\ \leq C_3 K^{\frac{1}{\rho+1}} (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N^{-1},$$

where C_3 is a positive constant (only depending on k).

Proof. We have

$$\sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} a(x)a(y)\mathfrak{a}(z) - \sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} a'(x)a'(y)\mathfrak{a}'(z) \\ = \frac{1}{N} \sum_{r \in \mathbb{Z}_N} \tilde{a}(r)\tilde{a}(-r)\tilde{\mathfrak{a}}(r) \left(1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{\mathfrak{b}}(r)^2 \right).$$

Let $\rho = k2^{k+3}$. If $r \in R \cap \mathcal{R}$, then by Lemma 6.7 of [5],

$$|1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{\mathfrak{b}}(r)^2| \leq 2^{15} \epsilon^2.$$

It follows that

$$\left| \sum_{r \in R \cap \mathcal{R}} \tilde{a}(r)\tilde{a}(-r)\tilde{\mathfrak{a}}(r) \left(1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{\mathfrak{b}}(r)^2 \right) \right| \\ \leq 2^{15} \epsilon^2 \sum_{r \in R \cap \mathcal{R}} |\tilde{a}(r)|^2 |\tilde{\mathfrak{a}}(r)| \\ \leq 2^{16} \epsilon^2 \min\{|R|, |\mathcal{R}|\}.$$

And by Lemma 2.6, we have $|R| \leq C'(\rho) \eta^{-\rho}$. Also, by the Hölder inequality, Lemmas 2.6 and 3.1,

$$\left| \sum_{r \notin R \cap \mathcal{R}} \tilde{a}(r)\tilde{a}(-r)\tilde{\mathfrak{a}}(r) \left(1 - \tilde{\beta}(r)^2 \tilde{\beta}(-r)^2 \tilde{\mathfrak{b}}(r)^2 \right) \right| \\ \leq 2 \sup_{r \notin R \cap \mathcal{R}} |\tilde{a}(r)\tilde{\mathfrak{a}}(r)|^{\frac{1}{\rho+1}} \left(\sum_{r \notin R \cap \mathcal{R}} |\tilde{a}(r)|^{2+\frac{1}{\rho}} \right)^{\frac{\rho}{\rho+1}} \left(\sum_{r \notin R \cap \mathcal{R}} |\tilde{\mathfrak{a}}(r)|^\rho \right)^{\frac{1}{\rho+1}} \\ \leq 2C'(2 + 1/\rho)^{\frac{1}{\rho+1}} C(\rho)^{\frac{1}{\rho+1}} K^{\frac{1}{\rho+1}} \eta^{\frac{1}{\rho+1}}.$$

□

Lemma 3.3. If $\epsilon^{|R|} \geq 2 \log \log w/w$, then $|a'(x)| \leq 2/N$ for any $x \in \mathbb{Z}_N$.

Proof. See [5, Lemma 6.3].

□

Let

$$A' = \{x \in \mathbb{Z}_N : a'(x) \geq \kappa/N\}, \quad \mathfrak{A} = \{x \in \mathbb{Z}_N : \mathfrak{a}'(x) \geq \kappa/N\}.$$

Then by the proof of Lemma 2.8 we have $|\mathfrak{A}| \geq (1 - 3\kappa)N$. By Lemma 3.3 we have

$$\frac{2}{N} |A'| + \frac{\kappa}{N} (N - |A'|) \geq \sum_{x \in \mathbb{Z}_N} a'(x) = \sum_{x \in \mathbb{Z}_N} a(x) \geq \frac{1}{3mK},$$

$$|A'| \geq \frac{N}{2} \left(\sum_{x \in \mathbb{Z}_N} a'(x) - \frac{\kappa}{N} \cdot N \right) = \frac{N}{2} \left(\sum_{x \in \mathbb{Z}_N} a(x) - \frac{\kappa}{N} \cdot N \right) \geq 2\kappa N.$$

Hence by Lemma 3.3 of [8],

$$\sum_{\substack{1 \leq x, y, z \leq N \\ x+y=z}} a'(x)a'(y)\mathfrak{a}'(z) \geq \sum_{\substack{x, y \in A', z \in \mathfrak{A} \\ x+y=z}} a'(x)a'(y)\mathfrak{a}'(z) \geq \frac{\kappa^3}{N^3} \nu_{A', A', -\mathfrak{A}}(0) \geq \frac{\kappa^6}{N}.$$

We may choose sufficiently small η and ϵ such that

$$\begin{aligned} \epsilon^{C(k2^{k+3})K\eta^{-k2^{k+3}}} &\geq \kappa^{-1} C_1 K w^{-\frac{1}{k(k+3)}}, \\ \epsilon^{C'(k2^{k+3})\eta^{-k2^{k+3}}} &\geq 2 \log \log w/w \end{aligned}$$

and

$$C_3 K^{\frac{1}{\rho+1}} (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) \leq \kappa^6/2.$$

So by Lemma 3.2, we have

$$\begin{aligned} &\frac{\phi(KW)^2(\log(KWN + \psi(b)))^2}{K^2 W^2 N^2} \sum_{\substack{x, y \in A, 1 \leq z \leq N \\ x \neq y, x+y=z}} \mathfrak{a}(z) \\ &\geq \sum_{\substack{x, y, z \in \mathbb{Z}_N \\ x+y=z}} a'(x)a'(y)\mathfrak{a}'(z) - C_3 K^{\frac{1}{\rho+1}} (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N^{-1} \\ &\quad - \frac{\phi(KW)^2(\log(KWN + \psi(b)))^2}{K^2 W^2 N^2} \sum_{1 \leq z \leq N} \mathfrak{a}(z) \\ &\geq \kappa^6 N^{-1} - C_3 K^{\frac{1}{\rho+1}} (\epsilon^2 \eta^{-k2^{k+3}} + \eta^{\frac{1}{k2^{k+3}+1}}) N^{-1} - N^{-\frac{3}{2}} \\ &\geq \frac{\kappa^6}{3N}. \end{aligned}$$

□

Acknowledgment. The second author thanks Professor Zhi-Wei Sun for informing the result of Khalfalah and Szemerédi.

REFERENCES

- [1] J. Bourgain, *On $\Lambda(p)$ -subsets of squares*, Israel J. Math., **67**(1989), 291-311.
- [2] J. Bourgain, *Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations. I. Schrödinger equations*, Geom. Funct. Anal., **3**(1993), 107-156.
- [3] P. Erdős and A. Sárközy, *On differences and sums of integers II*, Bull. Greek Math. Society, **18**(1977), 204-223.
- [4] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetical progressions*, J. d'Analyse Math., **31**(1977), 204-256.
- [5] B. Green, *Roth's theorem in the primes*, Ann. Math. (2), **161**(2005), 1609-1636.
- [6] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. Math., to appear.
- [7] A. Khalfalah and E. Szemerédi, *On the Number of Monochromatic Solutions of $x + y = z^2$* , Combinatorics, Probability and Computing, **15**(2006), 213-227.

- [8] H.-Z. Li and H. Pan, *Ternary Goldbach problem for the subsets of primes with positive relative densities*, preprint.
- [9] H.-Z. Li and H. Pan, *Difference sets and polynomials of prime variables*, preprint.
- [10] A. Sárközy, *On difference sets of sequences on integers I*, Acta Math. Acad. Sci. Hungar., **31**(1978), 125-149.
- [11] A. Sárközy, *On difference sets of sequences on integers III*, Acta Math. Acad. Sci. Hungar., **31**(1978), 355-386.
- [12] T. Tao, *The Roth-Bourgain Theorem*, preprint, unpublished.

E-mail address: lihz@sjtu.edu.cn

E-mail address: haopan79@yahoo.com.cn

DEPARTMENT OF MATHEMATICS, SHANGHAI JIAOTONG UNIVERSITY, SHANGHAI 200240,
PEOPLE'S REPUBLIC OF CHINA